IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 17-46
	)	
BRANDON COUGHLIN	)	

GOVERNMENT'S ANALYSIS OF THE SENTENCING CONSIDERATIONS IN 18 U.S.C. § 3553(A)

AND NOW comes the United States of America, by its attorneys, Soo C. Song, United States Attorney for the Western District of Pennsylvania, and Paul E. Hull, Assistant United States Attorney for said district, and respectfully submits this Analysis of the Sentencing Considerations in 18 U.S.C. § 3553 (a) as follows:

1. Nature, circumstances, and seriousness of the offense

The seriousness of these offenses cannot be overstated. This case involves a cyber-attack conducted by defendant, Brandon Coughlin, on a community health care entity (HCE). The circumstances of the cyber-attacks are described in the indictment and the Presentence report. Coughlin intended the September 18, 2013 attack to shutdown an HCE, who has since the early 1950's provided medical services to communities whose healthcare needs were underserved by then existing medical facilities. This HCE has strived to do good in the community all during its existence.

Coughlin's motive for this cyber-attack was pure spite. His intent was to shutdown the HCE's eleven locations throughout three Southwestern Pennsylvania counties. He succeeded.

Coughlin committed a series of computer intrusions of the HCE throughout the summer of 2013. His action culminated in a cyber-attack on the computer network that was at the heart of the HCE's operation on September 18, 2013. The cyber-attack disabled medical services at all eleven locations for at minimum four days. It further curtailed the provision of medical services for a much longer period of time because of the unavailability of medical records and lab and test results which were deleted during the attack. Because of the cyberattack, the HCE experienced system malfunctions for months after the cyberattack. The HCE still has been unable to recover 97,800 of the 326,000 medical record images related to various patients of the HCE that Coughlin deleted, even four years after the attack.

The 2013 cyberattack not only frustrated the provision of medical services to patients, but caused a financial harm to the HCE diverting money away from its mission of providing healthcare services.

Coughlin knew that the HCE was just beginning to improve the organization's cybersecurity. Indeed, the lack of fulltime onsite expertise was why the HCE hired him to work there, to bring the HCE's cybersecurity up to date over time. He knew that management

of the HCE was still unsophisticated in cybersecurity. In attacking the victim, he was doing the equivalent of targeting a vulnerable victim.

On December 16, 2016, the government obtained a recorded conversation wherein Coughlin was recorded discussing the HCE hack and other matters pertinent to the court's consideration of what sentence to impose. Coughlin said the following regarding the HCE hack:

> CHS (Confidential Human Source): So, I was hoping you could tell me the story what happened at the clinic and that-that might help me.
>
> [laughter]
>
> BC (Brandon Coughlin): So, the clinic you know why I did it right?
>
> [...]
>
> CHS: Well, yeah there's the Home Depot thing.
>
> BC: Right, so a few weeks after I got, you know, a few weeks after I got the job at the clinic they saw in the newspaper that Home Depot was, you know, in court with me.
>
> CHS: Um-hum
>
> BC: So, they basically forced me to resign. So, and again the woman who was in charge that was my boss didn't know shit-shit from anything. She wasn't an IT. So, I just literally created an account uh a dormant account.

BC: And then, you know, a month later or what not went in and fuckin' deleted eve-ry-thing! Formatted all their drives everything. …

BC: And um. So anyways I completely wiped them out. They took s-s . . . and I-I called them every day after, you know, seeing cause like "Hey, can I set up an appointment?". They would be like "sorry, we're closed, our computers are . . ." just to check to see how long it took them.

[laughter]

BC: It took them several weeks to get back up.

Coughlin's cyber-attack incapacitated healthcare resources for patients in three counties. His crime was a serious attack upon important healthcare infrastructure in Southwestern Pennsylvania.

2. History and characteristics of the defendant

2A. Coughlin's Education and Employment

Coughlin was well educated. He had an Associates degree at Southern Maine Community College and a Bachelors degree at Waynesburg University in computer related fields of study. He had the kind of education that would serve him well in a lucrative field for the rest of his life. However, the Information Technology (IT) field entails a position of trust because of the expertise needed and the access granted to mission critical systems of the employing organization. That trust can be misplaced. Coughlin used

his education to obtain employment at not only the HCE, but other companies such as DCK Worldwide, The Williams Company, and KBR Wiley through which he performed IT work for NASA Johnson Space Center in Houston, Texas as a contractor with full network access to critical computer systems at NASA.

2B. Character Trait for Vindictiveness

In this case, Coughlin became vindictive because he was forced to resign his position by the HCE. In discussing the FBI's investigation, Coughlin was recorded to say the following about his ethics and motive for attacking the clinic:

> CHS: Why don't they [FBI] just turn around and hire you?
>
> BC: Well I-you know should they-they-they just they need somebody who is ethics. Which girl if you put me on-if you put me on the good side my ethics should be good.
>
> [CHS sighs]
>
> BC: But.
>
> CHS: You went wrong with tryin' to proof a point.
>
> BC: Well.…
>
> CHS: You were in the wrong. You shoplifted at-at Home Depot.
>
> BC: Well yeah that's fine but they shouldn't have fired me at the clinic for-because of that.

He used the information gained from his former employment, his unauthorized access, and his information technology skills to

inflict great harm on the HCE because of this perceived slight. That flaw in character caused him to commit 2 crimes against the HCE in 2013 and 2014.

He was so intent on doing so that he used facilities at his subsequent IT positions with DCK Worldwide and The Williams Company as a platform to carry out his vindictive quest to punish the HCE.

2C. Harassment of HCE Personnel

Coughlin also harassed his replacement at the HCE, even though that person had no part in his involuntary separation from the HCE. On March 17, 2015, he sent a Valentine's Day card saying "Sending it with Love because You are You" with the handwritten inscription "forever & always yours" from a North Houston location. On or about April 15, 2015, he attempted to hack the LinkedIn page of the person who replaced him at the HCE. The owner of the LinkedIn account received notifications of two attempts to reset his password on the account. He found that shortly before the password reset attempts Coughlin was the last person to view his LinkedIn profile.

2D. Coughlin Committed Other Hacks

The government is aware that Coughlin's lack of ethics and his vindictiveness has lead him to carry out other hacking activities. First, Coughlin admits to engaging in hacking to harvest personally identifiable information. Second, the

government has evidence that Coughlin again hacked a former employer because he was fired.

Sanford School District Intrusion

Coughlin attended school in the Sanford School District in Maine. The CHS indicated that Coughlin told the CHS in prior conversations that he had gained computer access to the district's network to change his grades and access student and faculty personal information.

On or about December 16, 2016, the CHS recorded the following conversation with Coughlin concerning Coughlin's hacking of the Sanford School District in Maine from Texas:

CHS: But I'm too close to it.

BC: You are. I mean I'll tell you anyways but . . .

CHS: Like-like obviously if I-I would have said something already.

BC: Yeah

CHS: You know what I mean? So . . .

BC: Well okay so I was able to get into the Sanford public school district.

CHS: You told me that.

BC: From-from uh Texas and dumped their whole employee database. So, I literally have every teacher's social everything.

CHS: What?!

BC: Yeah

CHS: Are you-are you oh uh okay . . .

BC: Dumped it.

CHS: . . . dumped it. I thought you meant like deleted it. Okay.

BC: So, [M***] and I have went on several shopping sprees.

[laughter]

CHS: With just the social security number?

BC: We made fake IDs. Yeah [UI]

CHS: Oh my god Brandon! You're gonna' [sighs]. You are-you are getting bad.

[noise]

BC: Poor Mr. … [M***** M*****] got an eight thousand dollar Amazon card.

CHS: M***** . . . was he English?

BC: Social studies. Remember him?

[laughter]

BC: Or geography. Remember him?

CHS: Just-just pick a teacher you hate the most.

BC: I liked him. He was the one that spoke gay.

CHS: Oh, not him! Not him.

BC: But yeah so [noise] [UI] and I still have a lot of it. I have it all still.

CHS: Jeez

BC: But I think it was over a thousand.

CHS: Wow

BC: Employees.

…

[CHS makes noise]

ACT Pipe & Supply Inc. Intrusion

From approximately March 2015 through approximately November 4, 2015, Coughlin was employed at Act Pipe & Supply Inc. ("ACT"), as a Network Administrator. Matthew Wolfe, Senior Financial Manager of ACT and Hilary Tullier, Business Systems Manager of the IT department of ACT, explained the circumstances of the intrusion incidents at ACT. Shortly after Coughlin started at "ACT" there were issues with Coughlin not following directions, setting up unapproved remote access points, installing passwords and encryption on his work laptop, and creating his own network. After Coughlin was terminated from ACT on November 4, 2015, he was asked for the password to his work laptop. Coughlin refused to provide the password, rendering the laptop unrecoverable.

On November 6, 2015, an intruder entered ACT's system and harvested their password files. On November 19, 2015, the intruder entered their system and eight servers were destroyed, to include their email server; shared-drive server; and back-up server. The shared-drive connected 15 ACT sub-offices across Texas, causing IT

issues in all of their offices, from which it took months to recover. On March 19, 2016, an intruder used another contractor's account to destroy the virtual servers being rebuilt after the first intrusion. It took them approximately 6 weeks to recover from the second intrusion.

According to ACT, they have spent at minimum $50,000 in remediation. Additionally, since Coughlin's termination, his former supervisor has been repeatedly harassed on-line, has become the victim of identity theft, and has had credit issues.

On November 4, 2015, approximately 2 hours after Coughlin was removed from his position, someone, we believe to be Coughlin, deleted ACT company passwords in a company authorized web password storage vault (known as LastPass). Coughlin had been using it to store company passwords known only to him. Had he been successful, the System administrators at ACT would not have been able to access those computers. Ultimately, administrators were able to recover the deleted passwords. LastPass logs indicate that the Internet Protocol (IP) address used to enter the site to do the deletions was 73.32.59.182, which was a Comcast IP address we have found present in Coughlin's Amazon, Craigslist, Paypal, and eBay account records as the originating source IP address both before and after this deletion attempt.[1]

[1] LastPass logs show the use of IP address 73.32.59.182 to try to access LastPass on May 24, 2015, June 28, 2015, July 30, 2015, July 31, 2015, and November 4, 2015. Tullier indicated that Coughlin was the only company-authorized user of

Coughlin's actions demonstrate a callousness toward others. They clearly indicate that he is unsuited for the trust and responsibilities of an Information Technology position. His actions indicate that this Court must impose an appropriate jail sentence to deter him from further using his computer skills to cause harm.

3. The need to promote respect for the law
4. The need to provide just punishment for the offense
5. The need to deter the defendant from committing similar criminal conduct in the future
6. The need to deter others from committing similar criminal conduct
7. The need to protect the public from the defendant

A consideration of these factors clearly favors the imposition of a significant jail sentence. The crimes in this case were clearly the beginning of a series of crimes and wrongs committed by Coughlin. They reflect a desire not to conform his conduct to the requirements of the law. They also reflect a high degree of callous maliciousness, which motivated him to attempt to destroy the HCE's ability to serve its patients. His crime was a serious attack upon important healthcare infrastructure in Southwestern Pennsylvania. Under these circumstances, a sentence

---

LastPass. Some of these LastPass login attempts were subsequently followed by transactions where it appears Coughlin engaged in internet transactions on his own accounts from the same IP address. The use of this IP address correlated with his residence at 20051 Silver Rock Drive, Katy, Texas outside of Houston Texas. According to his NASA application, he started living there in March 2015 and stayed there until he moved on May 25, 2016.

of probation would not "… promote respect for the law" nor "… provide just punishment for the offense."

Moreover, the evidence demonstrates a pattern of criminal conduct: Coughlin becoming employed in the IT or other department of a company, gaining knowledge about the company's computer network, being involuntarily separated from the company, and then vengefully launching a cyberattack on the company. Given that Coughlin will always have cyber-networking skills that can be employed to cause havoc, it is important for the Court to impose a jail sentence sufficient to deter Coughlin from ever using his skills to conduct unauthorized computer intrusions and damage in the future.

Without such a sentence that deters him from this form of cyber-revenge, he poses a great risk of harm to future companies and employers where he will work. He also poses the same risk of harm to former employers, such as NASA. The sentence the court imposes must protect the public from Coughlin's penchant for conducting cyberattacks.

Cyberattacks are now a common plague on our way of life. They inflict harm and damage on individuals, commercial institutions, and on important infrastructure, such as healthcare entities. The frequency of such attacks is increasing. The sentence this Court imposes must also deter others from conducting such cyberattacks.

In this case, the goals of sentencing will only be served by a significant jail sentence, at the top of, or above the guideline range.

8. The kinds of sentences available
9. The applicable guideline range

In the government's view, the factors support the need to impose a lengthy sentence of imprisonment. The sentence of imprisonment should be large enough to address the nature and circumstance of the offense, its impact, the seriousness of the offense, the provision of just punishment which will promote respect for the law by the public, the protection of the public from further crimes by Coughlin, the need to deter Coughlin from further cyberattacks, and the need to deter others from future cybercrimes. The minimum necessary punishment in accordance with the application of these factors may necessitate a sentence at the top of the guideline range or above.

The government also submits that this Court should impose an occupational restriction barring Coughlin from employment as an Information Technology/Computer Network/Computer Forensic professional for any individual, business, organization, partnership, or corporation as a condition of any probation or supervised release this Court may impose for the length of the term of supervision that the Court may impose. Under certain conditions, this Court has the authority to impose an occupational

restriction as a condition of probation or supervised release. 18 U.S.C. §§ 3563 (b)(5) and 3583 (d).

Section 5F1.5 provides that occupational restrictions may be imposed only "to the minimum extent necessary to protect the public" as follows:

> Occupational Restrictions
>
> (a) The court may impose a condition of probation or supervised release prohibiting the defendant from engaging in a specified occupation, business, or profession, or limiting the terms on which the defendant may do so, only if it determines that:
>
> (1) a reasonably direct relationship existed between the defendant's occupation, business, or profession and the conduct relevant to the offense of conviction; and
>
> (2) imposition of such a restriction is reasonably necessary to protect the public because there is reason to believe that, absent such a restriction, the defendant will continue to engage in unlawful conduct similar to that for which the defendant was convicted.
>
> (b) If the court decides to impose a condition of probation or supervised release restricting a defendant's engagement in a specified occupation, business, or profession, the court shall impose the condition for the minimum time and to the minimum extent necessary to protect the public.

Guidelines § 5F1.5. In United States v. Smith, 445 F.3d 713 (3d Cir. 2006), the Court upheld a supervised release modification which barred defendant from employment with an attorney or law firm during his 3-year term of supervised release. Smith had been sentenced to 41 months on a wire fraud conviction involving nearly $600,000 in losses resulting from Smith's false representation

that he was a legal consultant with connections to Motorola. Smith also had prior convictions, which involved preparation of fraudulent court orders, forging attorneys' signatures and obtaining money through unauthorized practice of law. When, upon Smith's release from prison, attorneys offered to hire him, the Court granted the government's petition to preclude such employment. The Third Circuit determined the restriction imposed was authorized by § 3583(d)(2), which permits a district court "to impose occupational restrictions as a condition of supervised release, provided the restrictions 'involve[] no greater deprivation of liberty than is reasonably necessary' to promote criminal deterrence, protection of the public, and effective correctional treatment..." in accordance with 18 U.S.C. §3553 (a)(1) and (2).

The government submits that this memo and the Presentence report establishes that a direct relationship exists between Coughlin’s occupation and his hacking activities in this case; that a restriction is reasonably necessary because he has used his occupational skills to carry out other hacking activities in addition to these offenses; and that the proposed occupational restriction is reasonably related to the factors described in 18 U.S.C. §3553 (a)(1) and (2).

While the proposed occupational restriction will also ameliorate the risk to future IT employers, the Court should also

order that Coughlin shall not engage in unauthorized access to computer facilities of others and shall not possess passwords and other means of gaining unauthorized access to the computer facilities of others. This is necessary because Coughlin is still capable of conducting hacking activities outside of any employment.

10. The need to provide the defendant with educational or vocational training, medical care, or other correctional treatment

This is not a significant issue since Coughlin is well educated. He does not suffer from any particular medical or other issue, which the Bureau of Prisons cannot readily handle.

11. The need to provide restitution

Coughlin cannot repay fully the victim. We do not believe that Coughlin is truly likely to pay all the monies lost back to the victims, and the best way to make the victim feel that justice has been done is to show them that these crimes receive a serious punishment, so that Coughlin and others are deterred from victimizing others in the future.

WHEREFORE, the government respectfully requests that the court impose a lengthy sentence of incarceration.

Respectfully submitted,

SOO C. SONG
United States Attorney

/s/Paul E. Hull
PAUL E. HULL
Assistant U.S. Attorney
PA ID No. 35302